Interview with Vice Admiral Nancy E. Brown
Director for C4 Systems, The Joint Staff

Vice Adm. Nancy E. Brown

Vice Adm. Nancy E. Brown serves as the Director, Command, Control, Communications and Computer Systems (C4 Systems), the Joint Staff and as the Joint Community Warfighter (JCW) Chief Information Officer (CIO). In her dual capacity she is the principal advisor to the Chairman, Joint Chiefs of Staff on all C4 systems matters within the Department of Defense (DoD) and serves as an advocate for the link between combatant commanders C4 requirements and actions to deliver capabilities to meet their needs.

Since Vice Adm. Brown returned to the Joint Staff in August 2006, she published the Joint Net-Centric Operations (JNO) Campaign Plan (available at http://www.jcs.mil/j6/c4campaignplan/JNO_Campaign_Plan.pdf) to provide a unifying strategy to better integrate and synchronize joint community transformation and maximize joint warfighting capabilities.

This is an update to the first Joint C4 Campaign Plan, published in September 2004 by Marine Corps Lt. Gen. Robert Shea, the former Director C4 Systems, and incorporates new strategic guidance including the March 2006 National Security Strategy, the 2006 Quadrennial Defense Review Report, the 2006 Strategic Planning Guidance, the 16th Chairman's Guidance to the Joint Staff, and a new National Military Strategy for Cyberspace Operations. These documents detail the strategic direction of the Department and describe the net-centric capabilities to be employed by the joint force.

The plan also includes and builds on the significant progress in the development of net-centric concepts. Both the Net-Centric Environment (NCE) Joint Functional Concept and Net-Centric Operational Environment (NCOE) Joint Integrating Concept (JIC) were approved by the Joint Requirements Oversight Council (JROC). Their approval signifies the official Department support of the operational-level net-centric capabilities required to support contingencies across the continuum of military operations, key attributes necessary to compare capability solution alternatives and how future joint force commanders (JFCs) will employ net-centric capabilities. The NCOE program has evolved into Joint Net-Centric Operations (JNO). The next version of the NCE Joint Functional Concept will be titled the "JNO Joint Functional Concept" to reflect the ongoing work to refine capabilities in the net-centric area.

Finally, the plan focuses efforts over the next two to five years on the broad goals, specific objectives and achievable actions leading to full implementation of the capabilities that Joint Net-Centric Operations provides to the joint force in 2015. These actions include moves to address delivering capabilities incrementally to meet warfighter needs vice waiting to deliver full capabilities in the outyears.

CHIPS asked Vice Admiral Brown to discuss the Joint Net-Centric Operations Campaign Plan and other ongoing initiatives in support of the joint warfighter in March 2007.

CHIPS: How does the plan help the joint warfighter in assisting the Iraqi government in stabilizing the population and in nation building?

Vice Adm. Brown: The plan is focused on delivering capabilities to improve warfighter effectiveness. The primary initiatives under way include operationalizing cyberspace; addressing information sharing issues; driving changes to coalition networks; and tackling the spectrum management challenges our warfighters face in ongoing operations.

First in operationalizing cyberspace, my staff is leading efforts to provide better information assurance capabilities to the combatant commands, establish quality training for our cyberspace professionals, conduct annual cyberspace war games (for example, Bulwark Defender), and develop innovative national and military policy in this critical warfighting area.

Second, through the plan, my staff is sponsoring information sharing initiatives in support of coalition and interagency operations. Teaming with the Office of the Assistant Secretary of Defense for Networks and Information Integration, we are developing a DoD information sharing strategy and associated implementation plans to facilitate improved communications between DoD elements and with our non-DoD mission partners.

Third, in direct support of the war on terror, we are driving changes to our coalition networks enabling significant improvements in our ability to share information with allies, mission partners, other agency partners and nongovernmental activities.

Finally, we are addressing numerous spectrum management initiatives critical to warfighter effectiveness. We lack a joint spectrum management tool to do real-time spectrum planning, and spectrum allocation and deconfliction on the battlefield, not only between U.S. forces, but with our coalition partners and host nation authorities. Therefore, we have focused our efforts on providing staff support to the U.S. Central Command (USCENTCOM) and to the Joint Improvised Explosive Device Defeat Organization to help defeat the improvised explosive device threat.

We are also overseeing the development of both a near-term tool to assist in countering the IED threat and a future spectrum management tool suite to manage the electromagnetic (EM) spectrum used by the Department in a net-centric environment. Our near-term tool, the Coalition Joint Spectrum Management Planning Tool (CJSMPT), will deliver an integrated EM spectrum management and near-real time mission planning tool to enable frequency managers to perform EM spectrum planning and deconfliction from tactical through combined and joint task force levels.

CJSMPT will transition to become the baseline of our future spectrum management tool suite, called the Global Electromagnetic Spectrum Information System (GEMSIS).

CHIPS: Is the CJSMPT new or does it replace something?

Vice Adm. Brown: CJSMPT was in response to a Joint Urgent Operation Needs Statement from the warfighters to address immediate EM spectrum concerns. It builds on the concept of current tools but adds key functions that our warfighters do not have today, namely, advanced spectrum planning, real-time deconfliction and a visualization tool that provides a picture of actual spectrum use.

CJSMPT links to existing databases resulting in a more comprehensive spectrum knowledge repository establishing a common display warfighters can use in building their plan for spectrum allocation and use.

CHIPS: The associate director of the White House Office of Science and Technology, will be leading the U.S. delegation at the World Radiocommunications Conference in the fall to present both U.S. commercial and defense spectrum requirements. Has the Joint Staff already provided warfighter requirements?

Vice Adm. Brown: Yes, we have been involved in planning for WRC for about two years. We are engaged with other agencies ensuring warfighter requirements are represented in all formal U.S. positions. My staff is helping build the U.S. government position that becomes an input to the U.S. national position on a multitude of issues.

The U.S. government position incorporates inputs from government departments and agencies, while the national position also includes inputs from industry. My staff, along with the OSD staff, has been working in various governmental working groups and has presented a consolidated request articulating warfighter needs. In addition, we will have several DoD representatives in attendance supporting the delegation.

CHIPS: You were in Iraq in 2005 for an eight-month tour as the Deputy Chief of Staff for Communications and Information Systems for the Multinational Forces-Iraq working to establish an IT infrastructure. Has it been sustained?

Vice Adm. Brown: Unfortunately, the way we swap out forces, we tend to swap out everything. The Army calls it RIPTOA, which is Relief In-Place Transfer of Authority. The problem is — it really is ripping because they take everything out, and the new group brings everything with them. They build everything from the ground up every time. It has been difficult to establish an infrastructure that's enduring.

The USCENTCOM J6 has done a great job establishing policies and procedures and being ruthless in saying, 'That's not the way we are going to do it. We have an enduring infrastructure here. We have a set number of applications and systems that support the effort and when you come in, this is what you are going to use.' We are at a point now where we are starting to build on that, and this upcoming rotation is going to be much different than the rotations in the past.

CHIPS: Is the network you referred to earlier for coalition collaboration, CENTRIXS, or something else?

Vice Adm. Brown: We have about 17 different CENTRIXS networks. They are different because of the releasability of information and the different partners that are on the different versions.

Initially, we are talking about trying to collapse all of those into one network and to use rules-based software that would allow access and provide for the distribution of information. It would be based on identity and how the rules were established in the network that say what you can see and what you can't see.

Once we are able to collapse CENTRIXS, we hope we will be able to move all data presently residing on it into SIPRNET. The ultimate goal is to get to the point where we have one network with all the information stored in the same database, and it's tagged to the point where my identity allows me to go into that database and see only what I am authorized to see.

I say we can get there within the next few years.

CHIPS: Hasn't CENTRIXS improved over the years?

Vice Adm. Brown: CENTRIXS is not dynamic. It is not agile. It is not robust. If I want to add a new partner on CENTRIXS today, it's going to cost me, initially at least, a million and a half dollars, and it will take about six months to do the paperwork. CENTRIXS has improved, but it is still cumbersome. The CENTRIXS capability is the best we have today, but we need to do a lot better.

CHIPS: The plan discusses how DoD will transition from IPv4 to IPv6. Has progress been made in this area?

Vice Adm. Brown: Progress has been made in this area, although not substantive progress at the warfighter level. The Department laid out the key elements of its transition strategy including a requirement that procurements, acquisitions and developments be IPv6 capable, while continuing to be IPv4 capable — our current environment. To minimize costs, we are attempting to acquire IPv6 capabilities through scheduled technology refreshment activities.

My staff is supporting the development of the DoD IPv6 Integrated Implementation Schedule, which provides a consolidated schedule for major networks and programs that support combatant commanders, the Services and agencies.

We are also supporting the DoD IPv6 Master Test Plan which outlines a coordinated approach for DoD IPv6 testing. The test plan establishes the operational criteria that must be demonstrated during the transition to IPv6.

Finally, there are challenges we need to address in order to effectively transition to IPv6. First, we must ensure security is addressed before, during and after the transition. The development of IPv6 security tools must be accelerated. Second, the development of applications that showcase the benefits of IPv6 to the warfighter must also be accelerated. Third, we must address the perceived IPv6 performance degradation to ensure that as we transition, our investments are sound and will improve warfighter effectiveness.

As you can see, we are cautiously moving forward in this area.

CHIPS: Are you looking to industry to take the lead?

Vice Adm. Brown: Yes, we are looking to industry to share lessons learned and some of the issues they have tackled in transitioning to IPv6. The Defense Information Systems Agency has an IPv6 laboratory and project office. We are working closely with the Services and DISA to work through IPv6 issues and how we can mitigate them.

The transition from IPv4 to IPv6 must be seamless. We cannot afford to put at risk our current operational capabilities during this transition. We must maintain interoperability and security during and after the transition to IPv6 while continuing support for IPv4 legacy systems. We are also charged to provide the Chairman with a recommendation on the benefits and operational risks of going

Joint Staff Director for C4 Systems Vice Adm. Nancy Brown during the interview with CHIPS March 29, 2007. The admiral was in Virginia Beach, Va., for the day to participate in the Network Centric Operations Industry Consortium Plenary Meeting. The NCOIC mission is to facilitate global realization of the benefit inherent in net-centric operations.

to IPv6. Before DoD makes the leap, the Chairman has to certify that it's the right thing to do. We are working with DISA and the Services to mitigate risks and determine the key components of the Chairman's certification.

CHIPS: Will there be unique aspects to the application of IPv6?

Vice Adm. Brown: Yes, there are unique capabilities that IPv6 provides, such as expanded address space, enhanced quality of service, and expanded discovery of services, that will allow us to do more in a net-centric environment. However, before we declare victory, realize that IPv6 capabilities are in varying states of maturity in the areas of development, testing and delivery. We must have full situational awareness of enhancements in these areas in order for us to effectively collaborate with other federal agencies for the safe and economical adoption of this new technology. To fully leverage IPv6 capabilities, we must not lock ourselves into employing IPv6 in the same manner we employed IPv4.

Finally, we must take a long-term view to focus on what provides the greatest benefit to the warfighter and invest in proven capabilities that lay the foundation so that we can take advantage of capabilities as they evolve and mature.

CHIPS: Can you talk about the problems associated with maturing the Global Information Grid?

Vice Adm. Brown: The real challenge is to make the GIG relevant to the DoD information enterprise. We have to take on a data centric approach. The bottom line is: we have to get to the point where data is accessible to all users that require it, including unanticipated users. We will accomplish this through effective implementation of our data strategies and standards. When the enterprise gets this right, the communication infrastructure of the GIG can be resourced and maintained by the Services and DISA.

Another challenge to maturing the GIG is how to transition legacy equipment and applications to the GIG, while providing continued operations and maintenance of systems operational on the GIG. We are engaged with DISA to ensure joint warfighting capabilities are effectively incorporated into the Defense Information Systems Network, or DISN.

DISA is actively working with the Services and agencies to efficiently transition from legacy systems to emerging systems that facilitate joint network-centric operations. In addition, the Office of the Secretary of Defense, Program Analysis and Evaluation, is leading a working group to review the proposed investments for the DISN and to develop a way to finance the validated requirements.

The Joint Staff, various organizations within OSD, the Services and agencies are actively participating in this working group to identify what is required to sustain the network and meet the warfighter demands on the network as operations continue to become more net-centric.

CHIPS: What does "pervasive knowledge" mean in the plan?

Vice Adm. Brown: Pervasive knowledge is the result of effective knowledge sharing and can be described as the ability to permeate or spread information or thought throughout a group of individuals. Operating in a pervasive knowledge environment, users get information or knowledge at any place, at any time in the proper context.

Knowledge management is a mind-set enacted by people, enabled by process and enhanced by technology. Knowledge management processes help foster a culture of information sharing and help knowledge workers organize information and determine applicability to specific persons, organizations or processes. As derived from the NCOE JIC, knowledge management is the ability to systematically discover, select, organize, distill, share, develop and use information in a social domain context to improve warfighter effectiveness.

CHIPS: Can you give me an example of pervasive knowledge?

Vice Adm. Brown: Pervasive knowledge is having knowledge available wherever you are. My vision is that as a commander, I would walk into the command center and identify myself with either a fingerprint or my retina (whatever biometric is eventually chosen) but not a common access card, or something else I need to remember to take out of my wallet or switch out of my jeans to my suit. The source of my identification needs to be something that is with me all the time that identifies me dynamically and gives me the access I need wherever I am.

So I walk into the command center, and the command center is there to support the way I make decisions. I put in my fingerprint, I am recognized and automatically the screen and all the displays go to my personal requirements for the information I need in a way that I can synthesize it, and it allows me to make immediate decisions with the best quality information available — so that I can make sure that my force stays in front of the enemy in their decision process.

CHIPS: How far away are we from your vision?

Vice Adm. Brown: I think the technology is there to support at least 80 percent of the vision, but the culture is still a little bit farther away from being able to do so.

We have to get beyond the way we traditionally set up organizations and the way we structure information in an organization. We have to get to a point where it is not the J-2 who is holding all the Intel data and not sharing it, and the J-3 who has another set of data and the only way the commander gets an overall picture is

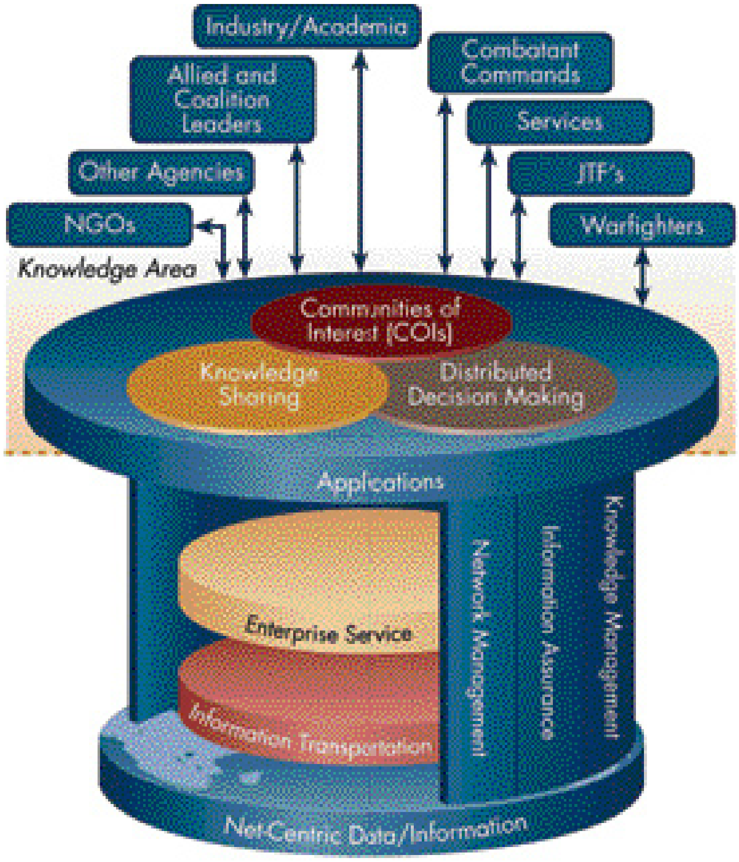

Figure 1. The Joint Net-Centric Operations Context as illustrated in the JNO Campaign Plan.

by taking what each one of the J-codes gives him or her and then synthesizing it themselves. *(An illustration of the JNO context of sharing knowledge and information in joint warfighting is shown in Figure 1. Figure 2, on the next page, shows JNO Observe-Orient-Decide-Act (OODA) Loop integration.)*

We must get to the point where an organization does not work in structured J-codes but in functional areas that synthesize the information and can put it all together — and when the commander needs it — it is decision-quality information.

CHIPS: The JNO calls for dynamically supported operations at every echelon, especially warfighters at the "first tactical mile." At that level of engagement how is the word getting out about what's available?

Vice Adm. Brown: Great question. I'll address it in two parts. To get the word to the warfighter, we need to ensure two things: processes are in place to ensure information can be appropriately discovered and that network connectivity exists so that the warfighter has timely access.

Historically, the communications and information community has not done a good job communicating how to access a wealth of information available to the warfighters via reach back or about our present efforts to move to a joint net-centric operational force. We have got to do a better job of demonstrating the operational relevancy and benefits of capabilities being delivered to the warfighters.

To get the word out, I recently published the J-6 Strategic Communications Plan – a tool to develop and communicate key messages throughout the Department, to industry, academia and any user or developer of joint net-centric capabilities for our warfighters.

We are working the gaps associated with delivering joint net-centric capabilities identified by the combatant commanders through their Integrated Priority Lists submissions and gaps identified through the JNO Joint Capabilities Document (JCD). Two of the net-centric 'Most Pressing Military Issues' are 'improve information sharing with mission partners' and 'improve information transport capabilities to enable joint forces in net-centric operations.' We are supporting efforts to the JROC to address these immediate warfighter needs.

The need to share information has been identified by seven of the nine combatant commanders. They require the ability to: share, collaborate and synchronize information with mission partners; extend sharing capabilities to mission partners; and provide exportable and affordable capabilities to less capable mission partners. The geographic combatant commanders continue to highlight the importance of this connectivity and are demanding further expansion of these capabilities.

The recent report of increases in hostile attempts to penetrate and disrupt our networks has highlighted the need for greater defense in depth and enterprise solutions to better protect sensitive information. The Enterprise Solutions Steering Group (ESSG), a joint forum with representatives from the Joint Staff, OSD, the Services, DISA, the National Security Agency and combatant commands, fields key information assurance tools that provide much needed computer network defense capabilities to the warfighter. In the past two years, the ESSG has fielded sensors, vulnerability assessment and remediation tools, antivirus/anti-spyware capabilities and host base security systems.

Another tool to address immediate warfighter needs is through the Command and Control Initiatives Program (C2IP). This program allows us to be more responsive to combatant commands emerging or emergency needs. I have some great people working on the answers to some of our most difficult problems. Solutions they recommend are often at the very cutting edge of technology or are so out of the box that an acquisition program to fund them in a three-year (normal) budgeting cycle just won't do.

Through C2IP, I'm able to put dollars where there are needs today for our warfighters to connect them. With our program, we are able to fund C2 solutions putting 21st century C2 solutions into Third World environments.

In addition, in remote locations in Central America where we daily fight the war on drugs and narco-terrorism, we've been able to fund programs to enable secure communications and reach back to forward deployed forces.

Finally, we were able to provide the Commander, Joint Task Force Horn of Africa (CJTF-HOA) with a Navy surface ship identification system – a program for Navy vessels to deconflict themselves from commercial traffic afloat. The CJTF-HOA J6 required this system to monitor ship traffic around the horn and through the choke point of the Strait of Hormuz.

This capability was critical to their ability to separate wheat from chaff as it pertains to drug, weapon and terrorist smuggling in and out of this troubled area. With minimal associated costs, we were able to meet the commander's needs in months versus years based on the traditional method for acquisition.

As you can see, we are using the campaign plan to address more than just doctrinal and training needs but operational and programmatic needs [as well] to deliver joint net-centric capabilities to meet warfighters needs.

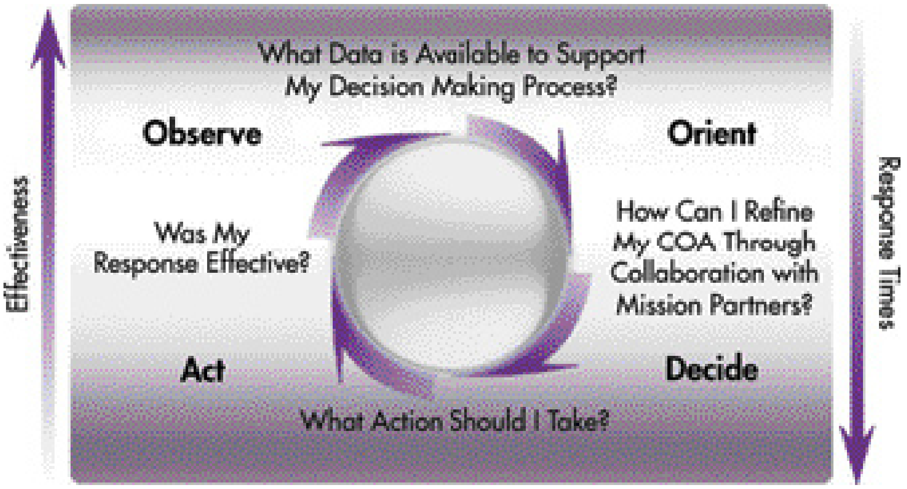
What Data is Available to Support My Decision Making Process?
Observe
Orient
How Can I Refine My COA Through Collaboration with Mission Partners?
Decide
What Action Should I Take?
Act
Was My Response Effective?
Effectiveness
Response Times

Figure 2. JNO-OODA Loop Integration.

Through JNO, warfighters will access secure information from both inside and outside their immediate environment and will ***observe*** *real-time events and receive feedback from previous actions.*

Through networking and synthesizing data from traditionally separate staff functions and collaborating with mission partners, warfighters will ***orient*** *on the unfolding situation, as the network responds to their changing operational needs.*

Due to the warfighter's access to information and knowledge, including the latest intelligence, surveillance and reconnaissance reports, the current operational picture and insights of subject matter experts and/or COIs, the warfighter will ***decide*** *on appropriate courses of action and will* ***act*** *with improved effectiveness.*

CHIPS: Is it a decision-support mechanism at the first tactical mile?

Vice Adm. Brown: What I'm really talking about is that today we design a system looking at people sitting in a building on robust fiber — and not the folks that are on the tactical side that are fighting the war or conducting the mission. These folks are for the most part disadvantaged users because of limited bandwidth, and not carrying large computers with them; only PDAs or laptops.

Also, a major aspect that would improve first tactical mile information sharing is through more effective situational awareness (SA) using a common operational picture (COP). The COP provides joint and coalition forces a clear advantage over hostile forces by quickly delivering a more accurate SA picture to any warfighter. The ability to continue receiving relevant, prioritized information, even during degraded operations, is also a major capability that future systems must take into account. We have to design systems that provide them the capabilities they need.

We have to look at it from the disadvantaged user perspective and not with the user that has an OC-12, or an Optical Carrier with a speed of 622.08 megabits per second, at their disposal in a huge computing facility. We must look at the person on the ship, not the carrier but the small boy, and look at the Soldier on the ground in a tank, and what capabilities that we need to provide to them.

CHIPS: Who should be reading the campaign plan?

Vice Adm. Brown: It's our intention that every user and developer of C4 and joint net-centric capabilities read the Joint Net-Centric Operations Campaign Plan. We have made it available to industry, combatant commands, the Services, agencies and interagencies on our Web site.

From CIOs and action officers to noncommissioned officers, the plan serves as a valuable tool to shape their perspectives of the JNO vision. The plan establishes the unifying strategy to better integrate and synchronize joint community transformational efforts in order to maximize warfighting capabilities in a net-centric environment. It is being used to establish a common framework within DoD to help define and describe processes for combatant commands, the Services and agencies that participate in capabilities validation, resourcing and acquisition. The plan sets the foundation for where the joint community needs to progress over the next two to five years to deliver joint net-centric operations.

CHIPS: I understand that you are interested in feedback. I read the campaign plan, and it's fascinating. But if I am a project leader, it doesn't tell me what I need to do to fit into the joint strategy.

Vice Adm. Brown: The campaign plan itself, the document, is high level, and it talks about goals. But if you go to the Web site, the specific actions that we believe support attaining those goals are listed. It tells you what we are doing, or who else is working on it and where we are in completing that action.

I can understand the comment that the campaign plan doesn't tell you exactly what you need to know, but if you go to the Web site [http://www.jcs.mil/j6/c4campaignplan/Annex_A_JNO_CampaignPlanOct06.pdf], and look under the goals and action items, there are over 120 action items that support the campaign plan. For each action item there is a point of contact.

CHIPS: The plan calls for collaboration with coalition partners to promote combined interoperability through standard policies and procedures. How will this be accomplished?

Vice Adm. Brown: The J6 is the designated DoD lead in several international forums to work collaboration for policy development, procedures and standards. Through NATO forums, the Combined Communications-Electronics Board (CCEB) and the Multinational Interoperability Council (MIC), my staff is able to influence coalition adoption of common policies, procedures and standards, as well as to adopt their best practices and lessons learned.

Joint net-centric operations transcends international boundaries, and J6 continues to partner with our NATO allies to bolster JNO capabilities. We are heavily engaged in NATO's Network Enabled Capability (NNEC) development. NNEC supports NATO's three transformation goals: decision superiority, coherent effects and joint deployment and sustainment. NNEC enables NATO's ability to conduct net-centric operations and supports information sharing among the NATO nations.

For my part, it is encouraging to see that NATO views net-centric operations and information sharing as we do. The NNEC effort is a positive step forward for developing both a strategy and roadmap that will enhance multinational information sharing activities. Through our collaborative efforts via the NATO Consultation Command, and Control (C3) Board, we will continue to improve those vital capabilities for coalition warfighters current and future.

CHIPS: Do you have to wait for funding for the new network capabilities that are specified in the plan?

Vice Adm. Brown: Currently, the Department has a number of large, key net-centric programs already funded that start delivering in the 2012 to 2015 time frame. We are looking at things we can do today, in the next couple of years, which give us some of those capabilities faster and allow us to start transforming before the 2012 to 2015 timeframe. There are certain things that need to be in place before those programs start delivering, such as policies and tactics, techniques and procedures that support those programs and technologies.

One method we have used to influence future network capabilities is our active participation in the DoD CIO's GIG enterprise-wide systems engineering efforts. It is critical that we, as the warfighting domain, set the operational context and priorities that establish these forward looking standards and performance metrics.

We have also started laying the foundation for changing how we do things so we can take advantage of the technology when it starts being delivered. We are synchronizing programs to ensure that as capabilities are delivered warfighters can use them immediately. For example, we have synchronized our space programs so that when we launch a Wideband Global Satellite Communications (WGS) system or Transformation Satellite Communications System (TSAT), the ground infrastructure is in place, and the Services have the terminals to use it.

A satellite is a big investment — and if you launch a satellite with nobody having a terminal that can use the satellite capability — you may be wasting valuable resources. The Department can't afford to do that.

CHIPS: The plan calls for specific actions within a two to five year time span. How will you measure progress?

Vice Adm. Brown: We use the campaign plan objectives and actions to continuously measure ourselves against our goals. This iterative process forces us to reevaluate our plan against the Chairman's priorities as well as the feedback we receive from the theaters and CIOs across the Department.

We use the plan to engage with the combatant commander J6s to identify and address strategic C4 issues affecting their ability to meet mission needs. As recently as February of this year, we gathered in Europe, hosted by European Command, to aggressively assess where we are with current initiatives. As a result, 16 new actions were added to the ongoing efforts to cover capability gaps.

We also brief high interest issues in the plan to the DoD CIO and C4 principals to gain consensus or vector checks on the actions in progress. This gives senior CIO and C4 leadership a chance to impact what we are doing.

Finally, the plan is a living document. My action group is working to develop appropriate metrics to measure our effectiveness. As such, key objectives and goals are briefed weekly allowing me to intercede on actions not moving ahead or that need vectoring. Upon completion of that review, the updated status of actions is posted on the J-6 Web site (SIPRNET only) for all stakeholders to review and provide comments or feedback.

CHIPS: With all your years in joint assignments, are you still active in the Navy Information Professional community?

Vice Adm. Brown: I am the senior Navy IP and the community sponsor. I take that very seriously and spend as much time as I can working on community issues and promotion plans and the assignment slates — and keeping track of where our folks are. When I travel, everywhere I go, I try to do an IP session so I get to see as many of the IPs as I can.

CHIPS: How many are in the community now?

Vice Adm. Brown: There are about 519 in the community. If we add in the limited duty officers (642X) and the warrants (742X), you'd get about 800 officers.

CHIPS: From what we hear from the IP community, they really enjoy their jobs.

Vice Adm. Brown: I think they do. We are a high-demand, low-density community. We are very much in demand, and there are not enough of us to go around. We have really taken on the Individual Augmentee mission. We have over 50 full-time yearly Individual Augmentee requirements, billets, in Iraq, Afghanistan, Horn of Africa and Guantanamo Bay.

Community-wise, there is a much higher percentage of IPs on the ground fighting the war than most of the other communities. When you look at our total inventory, we are a small community that delivers great dividends for the Navy and the joint community.

CHIPS: Do you see the community growing?

Vice Adm. Brown: I think the community has to grow a little bit. We have to figure out what the Navy needs from an information-based community in 2012. Are there other communities doing similar things? We need to take a look at this spectrum of communities that work in the information domain, what their skill sets are and what we think the Navy is going to need in 2012 and look to see if we have the right community construct in order to support that future requirement for the Navy.

As we work through that, there will be changes in community structure and the numbers for IPs may change — we may not be IPs any more. We may be called something else, or we may take on some functions from other communities, or there may be some consolidations.

I think there will be some change; I am not sure what it will be. We have an Integrated Process Team supported by Naval Network Warfare Command that is the Information Warfare community, formerly known as cryptologists, the Intel community, the oceanographic community, or 'METOCs,' and the IPs to see where there is synergy and where the differences are so great that you would not want to combine.

The question we must answer is, 'What is the best construct to meet the Navy's requirements for information-capable warriors?'

Visit the Joint Staff J-6 on the Web at http://www.jcs.mil/j6/index.html. To view Vice Adm. Brown's biography, go to http://www.jcs.mil/bios/bio_brown.html. To access the Joint Net-Centric Operations Plan go to the Joint Staff J6 Web site at http://www.jcs.mil/j6/c4campaign-plan/JNO_Campaign_Plan.pdf. CHIPS